UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
Criminal No. 17-CR-90 (PJS/DTS)

UNITED STATES OF AMERICA, Plaintiff, v. CHRISTOPHER GRUPE, Defendant.	)	**TRIAL BRIEF OF THE UNITED STATES**

The United States of America, by and through its attorneys Gregory G. Brooker, Acting United States Attorney for the District of Minnesota, Timothy Rank, Assistant United States Attorney, and Aaron Cooper, Trial Attorney, Criminal Division, respectfully submits its trial brief in the above-captioned case. Included in this memorandum is a summary of the facts the government expects the evidence will establish at trial, as well as briefing regarding possible evidentiary matters that may arise during trial.

I. OVERVIEW OF THE CASE

Canadian Pacific Railway (CPR) is a transcontinental railroad company headquartered in Alberta, Canada, with a 14,000-mile network of railroad tracks that passes through Minnesota and other parts of the United States. Computer network infrastructure for the CPR railroad is located in a variety of places, including an office in Minneapolis and another in Calgary. These computer networks control essential aspects of CPR's railroad line operations and communications. This case involves damage caused to those networks by a former CPR network engineer, defendant Christopher Grupe, using his unauthorized access to and insider knowledge of CPR's computer systems.

On December 15, 2015, following a twelve-day suspension, Christopher Grupe learned in a telephone call with CPR management that he was going to be fired. At his request, Grupe was instead permitted to resign. Grupe emailed a resignation letter to CPR shortly after the phone call, acknowledging that his resignation was effective that day, December 15, 2015. In the letter, he also promised to return all company property to CPR, including his laptop, remote access device, and access badges. But before he did, on December 17, 2015, Grupe used his laptop to remotely access the CPR network and, among other things, locked CPR out of two of its core switches—devices considered "network central" for all of CPR's major applications including rail traffic management and voice communications. Grupe did this by deleting several administrative-level accounts and changing passwords on the remaining administrative-level accounts. He also attempted to delete the network logs that had recorded his activity. Grupe's deletion and alteration of data on the switches was not immediately apparent to CPR, as the network appeared to be operating normally; however, had there been any significant problems with the CPR computer network, CPR IT staff would not have been able to access the switches to deal with the problem, potentially resulting in the shut-down of all railroad traffic.

The CPR network team discovered this damage on January 6, 2016, while trying to address a networking problem. CPR staff was unable to gain access to the two core switches and could not determine the cause. On January 7, 2016, CPR took the only available option and administered a shutdown to its core switches, in hopes that by rebooting the switches they could recover the passwords, despite a significant risk that the recovery process would not succeed. CPR did not know the extent of the damage to the switches, including whether the files that would allow them to recover the passwords had themselves been damaged, and so they did not know whether shutting down and rebooting the switches would in fact work. Fortunately, the procedure was successful and CPR was able to regain access to all of its network switches with minimal outage, albeit after the expenditure of substantial employee-hours dedicated to responding to and remediating the problem.

When it recovered access to the switches, CPR located the relevant network logs and traced the harmful activity to an internal IP address. Further analysis of the network revealed that the IP address had been assigned during that period to Christopher Grupe's laptop. Monitoring software on Grupe's laptop showed him logging into his laptop under his assigned "gru0040" username and opening up a remote connection to CPR's switches at the same time. Independent analysis by CrowdStrike, an outside incident response firm, confirmed these findings.

CPR experienced a financial loss of approximately $30,000 as a result of Grupe's conduct, consisting of time and labor of CPR employees and the cost of CrowdStrike's incident analysis. But if the network damage had not been discovered until a serious incident, or if the rebooting of the switches had not been successful in recovering access to the switches, the cost could have been much greater: conservatively, a system-wide rail stoppage for six to ten hours could have caused a loss in the millions of dollars.

On April 11, 2017, Grupe was charged in by indictment with one count of intentional damage to a protected computer, causing loss of more than $5,000.00, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i).

II. SUMMARY OF THE EVIDENCE AT TRIAL

A. CPR and its Computer Networks

Canadian Pacific Railway is a transcontinental railroad headquartered in Alberta, Canada, with 14,000 miles of railroad tracks spanning parts of Canada and the United States, including Minnesota. Each year, CPR transports millions of train carloads and logs billions of miles of travel. To keep all of its trains moving, CPR employs thousands of employees, including some employees who work out of its Minneapolis office at Canadian Pacific Plaza ("CP Plaza") at 120 South 6th Street.

During the 2015-2016 time frame, CPR relied in part on Cisco-manufactured switches – in essence, high-powered routers designed for large networks – to manage network communications for the entire railroad. These switches, known as "core" switches, were considered "network central" for all of CPR's rail traffic and communications, because they controlled, among other things, CPR train orders, signals, police communications, and train communications. Some of the switches were housed in CPR's Ogden facility in Calgary; others were housed at CP Plaza. Each "core" switch also contained other "virtual" switches that resided on the same physical chassis.

Grupe was hired by CPR in August 2013 to join its IT team at CP Plaza and began work that September. According to the resume he submitted to CPR, Grupe had prior experience in network engineering and IT infrastructure with large corporations, and technical expertise with Cisco Nexus 7k/5k switches, the same switches that were at the core of CPR's network.

As part of his employment, Grupe was one of a small number of IT staff granted administrative-level access to CPR's core switches – and Grupe was one of only a few of those with administrative-level access who actually accessed the switches, due to their sensitivity and the importance of the operations they controlled. Further, because of the sensitive nature of these computer systems, employees were admonished through a network banner that access to the CPR network was restricted to authorized users. Grupe was responsible for creating that banner.

Like other CPR employees, Grupe occasionally worked off-site. Therefore, CPR provided Grupe with a Dell laptop computer and a pre-configured remote access point ("RAP") for him to connect remotely to its network. The RAP provided an extension of the CPR computer network, allowing an employee to log directly into the CPR network from his or her laptop. That laptop – identified by its device name and MAC address[1] – would then be assigned an internally routable IP address through a Dynamic Host Configuration Protocol ("DHCP") server. Grupe's CPR username was "**gru0040**." His laptop ID was **7SCZH12**, and its MAC address was **b8:ee:65:58:54:f1**.

Because its employees would occasionally work off-site, CPR also used the services of a cybersecurity firm, CrowdStrike, to install and run monitoring software on laptops issued to CPR employees. Known as "FalconHost," the software would monitor end-point

[1] A MAC (or "Media Access Control") address of a computer is a unique set of alphanumeric characters assigned to the computer that is used to identify the computer on a network, such as a when connecting to a wireless router. MAC addresses are typically assigned by the manufacturer and are stored in its read-only memory.

activity on CPR devices in real time and report that information to a secure cloud environment.

B. The Nahant Yard Altercation

In December 2015, Grupe was assigned to a project at Nahant Yard, a CPR railyard located in Davenport, Iowa, which involved sensitive upgrades to the railyard's network. The upgrades were being coordinated by Cathy Mitchell, who was CPR's Project Manager for Data, and Rick Black, CPR's Project Manager for Telephony. Grupe was tasked with performing some preparatory work at the rail yard on December 1 and 2, and the network changes were scheduled to then take place on the evening of December 3. Mitchell had obtained authorization for the upgrades – called a "change window" – starting at 8:00 pm on December 3. A change window was required because the upgrades were going to result in a network outage for some period of time, which would have an impact on the Nahant Yard operations. On the evening of December 2, however, Ernest Seguin, CPR's Director of Network Architecture and Design Engineering, as well as Grupe's boss, learned from Rick Black that the phones at Nahant Yard had gone down because the network changes had not gone successfully. Seguin also learned that Grupe had begun the changes that day – one day ahead of the change window – without permission. Seguin, who was in Calgary, Alberta, assisted Grupe with restoring service, a process they were able to complete at about 1:00 am.

Midday on December 3, 2015, Seguin called Grupe about the unauthorized change and reminded him that proceeding with a network change without permission – and outside of the change window – was grounds for termination. Because Grupe had been unable to restore service on his own the previous night, and had needed Seguin's assistance to do so, they agreed that Seguin would assist Grupe during the change window that had been scheduled for that day at 8 pm.

That evening, at about 8 pm, Seguin returned to his office from a meeting with his supervisor, Tim Winn, and saw a 7:40 pm email from Grupe. In that message, Grupe said that he was going to proceed with the change on his own because he had tried to contact Seguin and Seguin had not responded. Seguin contacted Mitchell and learned that Grupe had already started the change and that the phones were down again.

When Seguin eventually got in touch with Grupe, he confronted Grupe about starting the change without him. Grupe became agitated, yelling and swearing at Seguin. When Grupe eventually calmed down, Seguin advised him that he would be suspended for insubordination and instructed him to turn in his CPR laptop the next day and not come in to work. Seguin also emailed Tim Winn, notifying Winn of the suspension and copying Grupe; Grupe responded within minutes, indicating that he was aware of the decision.

C. Grupe is Told he Will be Terminated but is Allowed to Resign Instead

Grupe was advised that he was not to access CPR property or use his CPR laptop during his suspension, except to submit an expense request related to his travel for the Nahant Yard upgrade. Grupe disregarded these instructions and returned to CPR's offices at CP Plaza several times over the following two weeks. Based on this, CPR determined that Grupe was not going to change his behavior and that he could pose a high risk to the business. CPR decided to terminate Grupe's employment.

On Tuesday, December 15, 2015, Seguin, Winn, and HR Director Patrick Price held a conference call with Grupe to inform him of his termination. During the discussion, Grupe asked if he could resign instead; this proposal was accepted by CPR. Grupe sent a resignation letter shortly after the call, effective that day, December 15, 2015. Grupe was further instructed to return all of his CPR assets – laptop, RAP, phone, and access cards – to CPR employee Fred Chambers. However, Grupe did not return any of this property to Chambers until the afternoon of December 17, 2015.

After Grupe returned the laptop, CPR was unable to turn it on. Ricardo Karel, a CPR Analyst, attempted to review the laptop, but was unable to retrieve any information – the laptop appeared to have been wiped.

D. CPR Discovers Damage to its Network

On January 6, 2016, CPR's network team encountered a serious problem the two of core switches at Ogden – devices that functioned as "network central" for all major applications at CPR including rail traffic management and voice communications. That morning, operations staff had discovered an issue in the network and needed to log in to the switches, but no one at CPR was able to gain access through the administrative credentials – they were locked out. This was a serious concern because if there were any problems with the CPR computer network, IT staff would not be able to address them; because so much of the operations of the railroad relied on the network, this would be especially problematic if there were an incident involving a train accident or other potentially catastrophic event. Accordingly, the IT staff went into "all hands on deck" mode to try to identify and correct the problem.

CPR IT staff contacted all CPR employees with administrative level access to the switches and no one was aware of any changes to the credentials. Because Grupe had worked on the switches while he was employed at CPR, he was contacted to see if he was aware of any issues; he denied knowing anything. Meanwhile, CPR consulted the manufacturer of the switches, Cisco, which advised CPR that there had been no system bugs or equipment issues that might cause this to occur.

Cisco also informed CPR that they could attempt to recover the administrative passwords by shutting down and rebooting the switches. This procedure would cause the switches to revert back to stored configuration files, which, if the procedure worked, would reset the passwords to their original settings. However, because they were locked out, CPR network engineers could not even determine if the systems would recover from a reboot; whoever had altered access to the switches could have deleted or altered the permanent configuration files as well.

On Thursday, January 7, 2016, CPR assembled a team and began the process of shutting down and rebooting the switches. As a precaution, IT staff was prepared to fully reprogram the configuration files on the switches in the event that they had they been altered or deleted. Fortunately, the rebooting procedure was successful, and access to the switches was eventually recovered with minimal outages. However, had CPR been locked out of these switches during a serious network incident, the resulting outage could have required them to shut down the entire railroad for at least six-to-ten hours. An outage of that length would have cost CPR at least two million dollars, excluding downstream costs to its customers or other railroads.

E. Investigation Reveals Grupe's Responsibility for Network Damage

Once access was regained, CPR employees retrieved "logs" from the compromised switches. The logs are time and date-stamped recordings of commands run on the switches that are stored in the memory of the switch. The logs showed that on the morning of December 17, 2015, a user who had been assigned the internal network IP address **10.188.206.220** gained access to multiple switches on the CPR network, made the unauthorized changes, and attempted to delete activity from the logs. Critically, the logs showed that the user had deleted administrative-level accounts and reset the password on two "core switches" – Ogden Core Switch 1 ("ognnxsw01") and Ogden Core Switch 2 ("ognnxsw02") – which controlled access to all of the switches in CPR's main datacenter. The log for Ogden Core Switch 1, for example, showed that the user with the internal IP address **10.188.206.220** changed the password on the "admin" account for that switch:

```
Dec 17 06:48:21 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=switchto vdc
ogncorsw01 (SUCCESS)
Dec 17 06:48:34 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=added
user:admin to the role:network-admin
Dec 17 06:48:34 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=updated v3
user : admin
Dec 17 06:48:34 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure
terminal ; username admin password 0 ******** role vdc-admin (SUCCESS
```

The log for Ogden Core Switch 2 showed, among other things, that the user with the internal IP address **10.188.206.220** deleted two administrative-level accounts ("cpadmin" and "arcnsparc") for that switch:

```
Thu Dec 17 09:08:37 2015:type=start:id=10.188.206.220@pts/1:user=admin:cmd=
Thu Dec 17 09:09:29 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted user cpadmin
Thu Dec 17 09:09:29 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted v3 user : cpadmin
Thu Dec 17 09:09:29 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; no
username cpadmin (SUCCESS)
Thu Dec 17 09:09:32 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted user arcnsparc
Thu Dec 17 09:09:32 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=deleted v3 user : arcnsparc
Thu Dec 17 09:09:32 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ; no
username arcnsparc (SUCCESS)
```

The log for Ogden Core Switch 2 also showed that, as with Ogden Core Switch 1, the user with the internal IP address **10.188.206.220** changed the password on the "admin" account for that switch:

```
Thu Dec 17 09:40:47 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=added user:admin to the
role:network-admin
Thu Dec 17 09:40:47 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=updated v3 user : admin
Thu Dec 17 09:40:47 2015:type=update:id=10.188.206.220@pts/1:user=admin:cmd=configure terminal ;
username admin password 0 ******** role vdc-admin (SUCCESS)
```

As noted above, internal IP addresses on the CPR network were assigned by the CPR DHCP server. A CPR employee retrieved the DHCP logs from December 17, 2015, which showed that the IP address **10.188.206.220** had been assigned to a CPR laptop with MAC address **b8:ee:65:58:54:f1** and device ID **7SCZH12** – the MAC address and device ID for the laptop in the possession of Christopher Grupe at the time the CPR switches had been accessed and the administrator accounts compromised.

CPR also engaged the services of CrowdStrike, a cyber-incident response firm to assist with identifying the source of the damage to its network switches and making sure CPR understood the full extent of the damage. CrowdStrike obtained logging data from its "FalconHost" monitoring application related to the device ID **7SCZH12**. Employee laptops issued by CPR contained FalconHost software that monitored activity on the laptop and stored it on servers controlled by CrowdStrike. The principal incident response analyst from CrowdStrike, Ryan Jafarkhani, reviewed the FalconHost logs, as well as the logs from the CPR switches. These logs showed the user "**gru0040**" – Christopher Grupe's username – logging in to Grupe's laptop on the morning of December 17, 2015, then gaining remote access to the CPR network and its compromised switches, deleting administrator accounts, and finally changing the network administrator accounts on two core switches.

Responding to and assessing the incident required approximately 125 hours of labor by CPR employees, costing CPR approximately 15-to-18 thousand dollars. In addition, CPR engaged the services of CrowdStrike to conduct an incident response investigation. CrowdStrike conducted its own analysis of the logging information from CPR and FalconHost and produced a report assessing the incident. CrowdStrike's analysis confirmed CPR's own internal review of the logs. CrowdStrike also provided recommendations to CPR for protecting against similar incidents in the future. CrowdStrike was paid 12 thousand dollars for its work.

III. POTENTIAL LEGAL AND EVIDENTIARY ISSUES

The government provides the following legal analysis concerning possible legal and evidentiary issues at trial.

A. Electronic Evidence

At trial, the government will seek to admit electronic evidence obtained during the course of the investigation. The electronic evidence includes server logs, emails, printouts, and other records obtained from CPR, CrowdStrike, and service providers. As set forth below, courts have held that this evidence is admissible under the Federal Rules of Evidence.

1. Logs

The government intends to introduce two categories of device logs: (1) logs that were automatically generated by switches and routers on the CPR computer network; and (2) FalconHost logs created by end-point monitoring software installed on the defendant's computer. These logs may be introduced in the form of original log text files or, when original log files are not available, as reproductions and excerpts of those logs embedded as text or picture images in emails or incident reports. Authentication and hearsay issues with respect to these logs are discussed below.

a. Authentication

As a general matter, the threshold for authenticity is no different for digital evidence than any other form of evidence. The foundational "requirement of authenticating or identifying an item of evidence" as a condition precedent to admissibility is satisfied by "evidence sufficient to support a finding that the matter in question is what the proponent claims it is." Fed. R. Evid. 901(a); *see United States v. Young*, 753 F.3d 757, 773 (8th Cir. 2014). Rule 901(a) only requires the government to make a prima facie showing of authenticity or identification "so that a reasonable juror could find in favor of authenticity or identification." *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) *See also United States v. Dhinsa*, 243 F.3d 635, 658 59 (2d Cir. 2001) (noting Rule 901 "does not erect a particularly high hurdle," and that hurdle may be cleared by "circumstantial evidence") (quoting *United States v. Ortiz*, 966 F.2d 707, 716 (1st Cir. 1992). Rule 901(b) further provides non-exhaustive "illustrations" of evidence that will satisfy this requirement.

Electronic evidence will be authenticated in this case through a variety of established means, as described below. Once the threshold showing has been met to admit the document, any questions concerning the genuineness of the item go to the weight of the evidence.

Witness With Knowledge: First, CPR network logs may be authenticated by CPR employees who obtained the logs from network devices under Federal Rule of Evidence 901(b)(1). Rule 901(b)(1) provides for authentication by testimony of a witness with knowledge "that an item is what it is claimed to be." For example, this permits authentication of emails by a witness who participated in the email communications. *See, e.g.*, *United States v. Safavian,* 435 F. Supp. 2d 36, 40 n.2 (D.D.C. 2006), *rev'd on other grounds*, 528 F.3d 957 (D.C. Cir. 2008). Likewise, it permits authentication of device logs by an individual with personal knowledge of the process through which the logs were obtained. *See, e.g.*, *United States v. Tank*, 200 F.3d at 630-31 (holding chatroom log printouts properly authenticated based on testimony of how logs were created); *United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997) (holding testimony of agent involved in printing out computer records sufficient to authenticate those records over defense argument that government failed to present a witness with personal knowledge of computer's operation or input/output accuracy).

A witness does not need to be a computer expert or have programmed the computer to authenticate data it produces. *See, e.g.*, *United States v. Moore*, 923 F.2d 910, 915 (1st

Cir. 1991) (citing cases); *United States v. Linn*, 880 F.2d 209, 216 (9th Cir.1989) (holding that witness's lack of knowledge of computer programming did not disqualify her as an authenticating witness for print out of computer records), *abrogated on other grounds by Florida v. White*, 526 U.S. 559 (1999). Instead, the witness simply must have first-hand knowledge of the relevant facts to which he or she testifies. *See generally Whitaker*, 127 F.3d at 601; *United States v. Miller*, 771 F.2d 1219, 1237 (9th Cir. 1985) (telephone company billing supervisor can authenticate phone company records); *Moore*, 923 F.2d at 915 (head of bank's consumer loan department can authenticate computerized loan data).

For CPR network switches and routers, CPR network engineers and analysts will testify to how the log files were extracted and, as in some cases, reproduced in email or screen image form. FalconHost logs can likewise be authenticated by CrowdStrike or CPR personnel who have familiarity with how the logs were obtained from the monitoring system and reproduced in email text or incident reports.

Comparison to Authenticated Evidence: Further, Federal Rule of Evidence 901(b)(3) allows authentication or identification by "comparison with authenticated specimens by an expert witness or trier of fact." *See, e.g.*, *Safavian*, 435 F. Supp. 2d at 40 (e-mail messages "that are not clearly identifiable on their own can be authenticated ... by comparison by the trier of fact (the jury) with 'specimens which have been [otherwise] authenticated'—in this case, those e-mails that already have been independently authenticated under Rule 901(b)(4)."). Accordingly, different forms of logs may be authenticated by way of comparison to other authenticated files.

Distinctive Characteristics: Records may also be authenticated by the introduction of testimony regarding their unique characteristics: *i.e.*, the "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." Fed. R. Evid. 901(b)(4); *see Young*, 753 F.3d at 773. Rule 901(b)(4) is "one of the most frequently used to authenticate email and other electronic records." *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 546 (D. Md. 2007); *see, e.g.*, *United States v. Fluker,* 698 F.3d 988, 999-1000 (7th Cir. 2012) (emails can be authenticated and connected to the sender by the testimony of the person receiving them, and by their content); *United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (emails authenticated by email address and contents of email, which were uniquely known to communicants); *United States v. Smith*, 63 F.3d 766, 770 (8th Cir. 1995) (documents authenticated by circumstantial evidence); *United States v. Bertram*, --- F. Supp. 3d ----, 2017 WL 1375184, *1-3 (E.D. Ky. 2017) (explaining authentication of emails based on unique characteristics by individuals other than sender or recipient). The logs in this case contain distinctive characteristics that satisfy Rule 901(b)(4), including time stamps, formatting and contents which reflect the fact they were obtained from CPR devices and FalconHost.

Weight versus Admissibility: Any defense claims that the electronic evidence is capable of being altered or modified should not preclude authentication and should be readily rejected. Questions concerning trustworthiness normally go to the weight of the evidence and not admissibility. As one court noted in dismissing a challenge to admit e-mails:

> The defendant argues that the trustworthiness of these e mails cannot be demonstrated, particularly those e mails that are embedded within e mails as having been forwarded to or by others or as the previous e mail to which a reply was sent. The Court rejects this as an argument against authentication of the e mails. The defendant's argument is more appropriately directed to the weight the jury should give the evidence, not to its authenticity. While the defendant is correct that earlier e mails that are included in a chain—either as ones that have been forwarded or to which another has replied—may be altered, this trait is not specific to e mail evidence. It can be true of any piece of documentary evidence, such as a letter, a contract or an invoice. Indeed, fraud trials frequently center on altered paper documentation, which, through the use of techniques such as photocopies, white out, or wholesale forgery, easily can be altered. The possibility of alteration does not and cannot be the basis for excluding e mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents). We live in an age of technology and computer use where e mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world. The defendant is free to raise this issue with the jury and put on evidence that e mails are capable of being altered before they are passed on. Absent specific evidence showing alteration, however, the Court will not exclude any embedded emails because of the mere possibility that it can be done.

Safavian, 435 F. Supp. 2d at 41.

b. Hearsay

"Hearsay" is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. Fed. R. Evid. 801(c). A "statement" is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion. The logs are not barred under the hearsay rules on two grounds: first, they are not by a "person" and, second, they do not contain assertions made for their truth.

Computers are not a "Person": First, hearsay is defined as an assertion or conduct by a "person," Fed. R. Evid. 801(a), (b), and therefore courts have widely recognized that computer-generated data are not hearsay. *See, e.g.*, *U.S. v. Lizarraga-Tirado*, 789 F.3d 1107, 1109-10 (9th Cir. 2015) (Google Maps "tack" representing GPS location was auto-generated by Google systems and therefore non-hearsay); *United States v. Lamons*, 532 F.3d 1251, 1263 (11th Cir. 2008); *United States v. Moon*, 512 F.3d 359, 362 (7th Cir. 2008); *United States v. Washington*, 498 F.3d 225, 230 (4th Cir. 2007); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) ("nothing 'said' by a machine . . . is hearsay"). Because CPR network logs and the FalconHost monitoring system logs are automatically generated by computers – not a "person" – they do not constitute hearsay.

No Assertions for "Truth": Second, these logs are not being introduced for the truth of any matter "asserted." An "assertion" "has the connotation of a positive declaration," *United States v. Lewis*, 902 F.2d 1176, 1179 (5th Cir. 1990) or, alternatively, represents "an expression of fact, condition or opinion." *State v. Kutz*, 267 Wis. 2d 531, 560 (Wis. Ct. App. 2003). Computer logs do not constitute any sort of assertive statement. Rather, like the dialing of a phone number or input of a PIN code into an ATM, they are merely non-assertive registers that will be introduced to show the inputs made to CPR devices and the resulting device outputs. *See, e.g.*, *United States v. Hamilton*, 413 F.3d 1138, 1142 (10th Cir. 2005) (computer-generated "header information" not hearsay because no "statement" made); *United States v. Bellomo*, 176 F.3d 580, 586 (2d Cir. 1999)

("Statements offered as evidence of commands or threats or rules directed to the witness, rather than for the truth of the matter asserted therein, are not hearsay."); *Safavian*, 435 F. Supp. 2d at 44 (holding that portions of e-mail communications that make imperative statements instructing defendant what to do, or asking questions are nonassertive verbal conduct that does not fit within the definition of hearsay).

2. Emails

The government also intends to introduce several items of email correspondence. Some of these emails represent communications among CPR employees other than the defendant; other of these emails represent communications to or from the defendant.

a. Authentication

As discussed above, these emails may be authenticated by testimony of the authoring or receiving witness, who has personal knowledge as to the email. They may also be authenticated by a witness with sufficient familiarity with the distinctive characteristics of the emails, as discussed above. Finally, they may be authenticated as business records, which were maintained by CPR

b. Hearsay

With respect to the bar on hearsay, the emails are admissible because (1) they will be used for non-hearsay purposes; (2) they represent party-opponent statements; or (3) they contain statements that satisfy an established hearsay exception.

Non-hearsay Purpose: Statements introduced for a non-hearsay purpose—*i.e.*, for something other than the truth of the assertion—do not violate the hearsay rule. *See, e.g.*, *Anderson v. United States*, 417 U.S. 211, 219 (1974) ("Out of court statements constitute hearsay only when offered in evidence to prove the truth of the matter asserted."). For example, instructions, commands or statements to demonstrate effect on or knowledge of the recipient are admissible. *United States v. Wright*, 739 F.3d 1160, 1170-71 (8th Cir. 2014). So too is "legally operative verbal conduct." *United States v. Pang*, 362 F.3d 1187, 1192 (9th Cir. 2004) (checks not barred by hearsay rule). Accordingly, emails and other communications by CPR employees may be introduced for the following non-hearsay reasons, among others: to show that Grupe knew he was suspended; to document that Grupe was told not to access the CPR network or show up at work; and to show that he resigned.

Statements by Party-Opponent: Email communications from the defendant – or including his statements – are admissible as statements by a party opponent under Fed. R. Evid. 801(d)(2)(A). Courts have regularly admitted the statements of a defendant contained in e-mail or chat communications under this Rule. *See, e.g.*, *United States v. Burt*, 495 F.3d 733, 738 (7th Cir.) ("[t]hose portions of the chat which represent [defendant] Burt's writings were properly admissible as admissions by a party opponent under Fed. R. Evid. 801(d)(2)"); *Siddiqui*, 235 F.3d at 1322 (11th Cir. 2000) (noting the e-mails "sent by Siddiqui constitute admissions of a party pursuant to Fed. R. Evid. 801(d)(2)(A)"); *Safavian*, 435 F. Supp. 2d at 43 (The [e-mail] statements attributed directly to Mr. Safavian come in as admissions by a party opponent under Rule 801(d)(2)(A) of the Federal Rules of Evidence."). Thus, emails and other statements by the defendant may be introduced for their truth. For example, his resume may be introduced to show his expertise with Cisco switches and his resignation email may be introduced to show that he had resigned from CPR on December 15, 2015, and understood that he was to return his CPR assets that day.

Context: The statements of others contained in email threads or chat conversations may be admitted not for the truth of the matter but as non-hearsay to supply context. *See, e.g.*, *Burt*, 495 F.3d at 738-39 (in Yahoo! chat communication involving the defendant and a third party found on the defendant's computer, the portion from the third party was admissible as non-hearsay and provided context to the conversation); *United States v. Dupre*, 462 F.3d 131, 136-37 (2d Cir. 2006) (in wire fraud prosecution, emails from investors demanding information about defendant's fraudulent scheme were not hearsay when offered not for truth of the assertion that the scheme was fraudulent, but to provide context for the defendant's message sent in response and to show defendant's knowledge).

Business Records: The government may also rely on established hearsay exceptions. Most importantly, the government will rely on the business records exception to the hearsay rule, which applies to a record of an act, event, condition, opinion or diagnosis, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the record, all as shown by the testimony of the custodian or other qualified witness. Fed. R. Evid. 803(6).

This rule encompasses system-generated logs maintained by a company as part of its business practices. *See, e.g.*, *United States v. Brooks*, 715 F.3d 1069, 1079 (8th Cir. 2013) (holding that business records exception applied to GPS data company routinely kept on its servers). Further, "in the context of electronically-stored data, the business record is the datum itself, not the format in which it is printed out for trial." *United States v. Keck*, 643 F.3d 789, 797 (10th Cir. 2011); *accord United States v. Nixon*, 694 F.3d 623, 634 (6th Cir. 2012). Accordingly, Grupe's expense report, which was maintained on CPR's servers; access logs for CP Plaza, which were maintained by CPR's servers; and subscriber records maintained by Microsoft and Comcast all qualify as business records.

B. Summary Charts and Demonstrative Exhibits

The government may utilize summary charts to represent voluminous computer data in lieu of presenting the underlying data to the jury. Summary charts of this nature are permitted under Fed. R. Evid. 1006, provided that "the charts 'fairly summarize' voluminous trial evidence; (2) they assist the jury in 'understanding the testimony already introduced'; and (3) 'the witness who prepared the charts is subject to cross-examination with all documents used to prepare the summary.'" *United States v. Green*, 428 F.3d 1131, 1134 (8th Cir. 2005) (quoting *United States v. King*, 616 F.2d 1034, 1041 (8th Cir. 1980)). Moreover, summary charts "may 'include assumptions and conclusions, but said assumptions and conclusions must be based upon evidence in the record.'" *Id.* (quoting *United States v. Wainright*, 351 F.3d 816, 821 (8th Cir. 2003)). Pursuant to Rule 1006, the government intends to introduce summary charts of exhibits CPR switch logs and other summary exhibits that correlate these logs with FalconHost and DHCP server logs.

Dated: September 20, 2017

Respectfully Submitted,

GREGORY G. BROOKER
Acting United States Attorney

s/ Timothy C. Rank

BY: TIMOTHY C. RANK
Assistant U.S. Attorney

AARON R. COOPER
Trial Attorney, Criminal Division